Keep your money safe

Surrey and Sussex Police Fraud Newsletter May 2020

Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.

Detective Chief Inspector Andy Richardson, Surrey Police & Sussex Police Economic Crime Unit

Be 'Cyber Aware' of online crime

As the country continues to rely more on technology, cyber experts are reminding us of the ways we can protect ourselves from online criminals.

The Cyber Aware campaign encourages people to **'Stay home. Stay Connected. Stay Cyber Aware'**, and its top tips for staying secure online are:

1. Turn on two factor authentication for important accounts
2. Protect important accounts using a password of three random words
3. Create a separate password that you only use for your main email account
4. Update the software and apps on your devices regularly (ideally set to automatically update)
5. Save your passwords in your browser
6. To protect yourself from being held to ransom, back up important data

If you're not sure how to do any of those things, the Cyber Aware website is a useful resource with lots of easy-to-understand help. The website can be found here: https://www.ncsc.gov.uk/CyberAware

Keep your money safe

Report suspicious emails to the National Cyber Security Centre (NCSC): report@phishing.gov.uk

The NCSC has launched a pioneering service for the public to report suspicious emails, including those claiming to offer services related to coronavirus.

Please forward any suspicious emails – including those claiming to offer support related to COVID-19 – to **report@phishing.gov.uk**. The NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately, helping to stop offenders in their tracks.

If you have lost money, please tell your bank and report it as a crime to Action Fraud as normal.

Protect yourself against 'sextortion' emails

We've seen a significant number of 'sextortion' cases across both counties in recent weeks, with most people receiving an email worded in the same way, indicating this is a phishing attempt on a mass scale.

Victims receive an email in which the sender includes the victim's password, and then suggests they have put malware onto the victim's device and have recorded the victim looking at pornographic material.

The fraudster demands a payment of $1900 in Bitcoin within 24 hours, threatening to share the video with the victim's friends, family and employers if they do not make the payment.

The best way to prevent this is to follow the Cyber Aware advice we shared on the first page of this newsletter, in particular setting a strong password, including a separate one for your main email account and setting up two factor authentication which adds an additional layer of security to your online accounts.

Buying pets online

In Sussex there have been two cases of people falling victim to an online ad for puppies and kittens, with the seller using the current lockdown as reason the victim can't come and see the animal. Photos are provided and the victim is persuaded to make payment in advance. The pet isn't ever delivered. When shopping online always:

- Use PayPal or a credit card to pay because both offer extra protection
- Research sellers carefully and check their terms and conditions and returns policy
- Remember our message that if something feels wrong, or too good to be true, it probably is

Roofing work, hedge and tree cutting: Don't be pressured by doorstep callers

Sadly vulnerable people continue to be targeted by doorstep fraudsters offering to do household jobs. In one recent example, a criminal offered to cut the top of an apple tree.

Keep your money safe

After examining the tree, he claimed it was diseased and tried to charge £225 to treat it, with what was later found to simply be water.

Protect yourself

- Always ask for identification before letting anyone you don't know into your house.
- Check credentials, including a permanent business address and landline telephone number. The mobile phone numbers given on business cards are often pay-as-you-go numbers which are virtually impossible to trace.
- Take control by asking the questions. Ask for references from previous customers or to see examples of their work.
- Don’t sign on the spot – shop around and ask friends or relatives for advice. Get at least three written quotes to make sure you’re not being ripped off.
- If in any doubt, ask the person to leave or call Consumer Direct on 08454 04 05 06. (Consumer Direct works in partnership with local trading standards teams).

How you can help us

If you or someone you know is vulnerable and has been a victim of fraud call:

Surrey Police on 101 or visit www.surrey.police.uk
Sussex Police on 101 or visit www.sussex.police.uk

Report fraud or attempted fraud, by contacting Action Fraud at http://www.actionfraud.police.uk/report_fraud or call 0300 123 2040